

REMARKS

Claims 64-86 are pending in the present application. In the above amendments, claims 66, 70, 72, 76, 77, 81, 82 and 86 have been amended.

Applicants respectfully respond to this Office Action.

Claim Objections

Claims 70 and 72-86 were objected to for various informalities. Claims 70, 72, 76, 77, 81, 82 and 86 have been amended, as requested, to address the respective informalities.

Claim Rejections – 35 USC § 112

Claims 66 and 72 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite. Claim 66 has been amended to eliminate the cost of an unauthorized user as compared with a value of a short term key. Claim 72 has been amended to delete “the integrated circuit” from lines 12-13. Accordingly, the rejections of claims 66 and 72 under 35 U.S.C. §112, second paragraph, should be withdrawn.

Claim Rejections – 35 USC § 103

Claims 64-69, 71-75, 77-80 and 82-85 were rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over U.S. Patent Application Publication No. 2002/0141591 to Hawkes et al. (the Hawkes application publication) in view of U.S. Patent Application Publication No. 2006/0168446 to Ahonen et al. (the Ahonen application publication). Claims 70, 76, 81 and 86 were rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over the Hawkes application publication in view of the Ahonen application publication, and further in view of Applied Cryptography, Second Edition by Bruce Schneier (the Schneier publication).

The rejection of claim 64 as allegedly unpatentable over the Hawkes application publication in view of the Ahonen application publication is respectfully traversed. Claim 64 recites a method for broadcasting encrypted multimedia content from a content provider to a plurality of authorized terminals over the air, comprising: each terminal forwarding a unique public key over the air to the content provider, wherein each terminal has a mobile equipment

and has a secure processing unit that securely stores a unique private key, corresponding to the unique public key, that is not accessible to a terminal user, and wherein the content provider encrypts a broadcast access key with each of the unique public keys to authorize a terminal having the secure processing unit securely storing a corresponding unique private key to receive the encrypted multimedia content.

The Examiner observes that the Hawkes publication “lacks each terminals forwarding a unique public key over the air to the content provider and lacks wherein the secure processing unit stores a unique private key (instead of Hawkes’s RK), corresponding to the unique public key.” See, Office Action, page 7. Applicants assert that the Hawkes publication also fails to disclose “wherein the content provider encrypts a broadcast access key with each of the unique public keys to authorize a terminal having the secure processing unit securely storing a corresponding unique private key to receive the encrypted multimedia content” (emphasis added). Applicants assert that the Hawkes application publication discloses encrypting a broadcast access key with a registration key RK. See, e.g., Figure 7B, step 426. In the Hawkes publication, the registration key RK is a shared secret key which is distinct from a public key having a corresponding private key. See, paragraphs [0038] and [0070].

The Examiner asserts that the Ahonen application publication remedies the disclosure deficiencies of the Hawkes application publication stating, “Similar to Hawkes RK, the private key that corresponds to the forwarded unique public key in Ahonen is used to decrypt a received encrypted key encrypting key (KEK), which is similar to Hawkes BAK (¶41).” See, Office Action, page 7. Applicants respectfully disagree with the Examiner’s assertion the key encrypting key (KEK) is similar to Hawkes BAK. The key encrypting KEK is unique to the subscriber, and the subscriber’s KEK is unicast to the subscriber. See, Ahonen, paragraphs [0009] – [0011]. In contrast, Hawkes broadcast access key BAK is common to a group of subscribed users, and the common BAK is encrypted by the user unique registration key RK. See, Hawkes, paragraph [0070]. Thus, Applicants assert that the KEK of Ahonen corresponds to the registration key RK of Hawkes, and not to a broadcast access key as recited in claim 64.

Further, with respect to modifying Hawkes to store a unique private key instead of a registration key RK, the Examiner asserts that “One of ordinary skill would have been motivated to perform this modification to achieve a simple mechanism for key dissemination, as taught by

Ahonen (¶7). See, Office Action, page 7. However, the Examiner ignores the contrary teachings of the Hawkes application publication in making this conclusion. The Hawkes application publication expressly teaches, "While public-key cryptographic methods solve a critical aspect of the 'key-exchange problem', specifically their resistance to analysis even with the presence a passive eavesdropper during exchange of keys, they do not solve all problems associated with key exchange. In particular, since the keys are considered 'public knowledge,' (particularly with RSA) some other mechanism is desired to provide authentication, as possession of keys alone (sufficient to encrypt messages) is no evidence of a particular unique identity of the sender, nor is possession of a corresponding decryption key by itself enough to establish the identity of the recipient." See, paragraph [0050]. The Ahonen application publication expresses similar concerns, "In any service making use of LKH, an important consideration will be the authentication of users so that the TEK is distributed only to authenticated users. Authentication can be done manually. For example, a subscriber to a service could call the service provider, pay a fee using a credit card, and receive a passcode. The subscriber enters the passcode into his terminal; and this is sent to the GC (e.g. encrypted with a public key owned by the GC. Another possibility is the use of Public Key Infrastructure (PKI) procedure, where a subscriber receives a certificate verifying that he is authorised to use the service, and verifying that the public key contained in the certificate belongs to that subscriber. The certificate is sent to the GC as part of the registration procedure. However, both of these procedures require considerable effort, and are not necessarily suitable for informal communications which are either short term or informal." See, paragraph [0012].

In contrast, Applicants recognized that "Provisioning of an access key such as BAK using the public cryptosystem as described eliminates a need for provisioning pre-shared secret key such as RK or TK, which can often involve complex procedures." See, specification, page 16, lines 23-29. Applicants respectfully assert that Examiner has not presented substantial factual basis, beyond the disclosure of Applicant's specification, to support the statement that "One of ordinary skill would have been motivated to perform this modification to achieve a simple mechanism for key dissemination". In analyzing the issue of obviousness, it is necessary to guard against slipping into the use of hindsight, and to resist the temptation to read into the prior

PATENT

art the teachings of the invention at issue. See, Graham v. John Deere Co., 383 U.S. 1, 36 (1966).

For these reasons, Applicants respectfully assert that claim 64 recites patentable advances over the Hawkes application publication in view of the Ahonen application, and respectfully request the rejections of claim 64 be withdrawn.

It is respectfully submitted that dependent claims 65-69 and 71 are at least allowable for the reasons given above in relation to independent claim 64.

Claims 72-75, 77-80 and 82-85 are integrated circuit, machine readable medium, and apparatus claims having features defined by language similar to that of method claims 64-69 and 71. Accordingly, for the reasons recited above with respect to claims 64-69 and 71, claims 72-75, 77-80 and 82-85 define patentable advances over the Hawkes application publication in view of the Ahonen application, and the rejections of claims 72-75, 77-80 and 82-85 should be withdrawn.

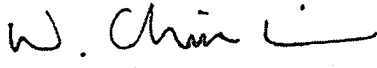
The rejections of claims 70, 76, 81 and 86 as being unpatentable over the Hawkes application publication in view of the Ahonen application publication, and further in view of the Schneier publication, are respectfully traversed. Claims 70, 76, 81 and 86 incorporate all of the features of independent claims 64, 72, 77 and 82, respectively. Applicants assert that the Schneier publication fails to remedy the disclosure deficiencies of the Hawkes and Ahonen patent publications as described above with respect to claim 64. Accordingly, Applicants respectfully request the Examiner to withdraw the rejections of claims 70, 76, 81 and 86.

REQUEST FOR ALLOWANCE

In view of the foregoing, Applicants submit that all pending claims in the application are patentable. Accordingly, reconsideration and allowance of this application are earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: January 22, 2009

By: 
Won Tae C. Kim, Reg. # 40,457
(858) 651 - 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502